UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/016,078	12/13/2001	Joey Eugene Whelan	01-5001	6937

32127 7590 05/27/2005

VERIZON CORPORATE SERVICES GROUP INC.
C/O CHRISTIAN R. ANDERSEN
600 HIDDEN RIDGE DRIVE
MAILCODE HQE03H14
IRVING, TX 75038

EXAMINER	
ELMORE, JOHN E	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 05/27/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/016,078	WHELAN, JOEY EUGENE	
	Examiner	Art Unit	
	John Elmore	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 December 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19,21-23,25,27 and 28* is/are rejected.

7)☒ Claim(s) *20,24 and 26* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *31 December 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *12/31/2001*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-28 have been examined.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. **Claims 1-19, 21-23, 25, 27 and 28 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Hirano et al. (US 2001/0004736A1), hereafter Hirano, in view of Rhoades (US 5,822,436).

Regarding claim 1, Hirano teaches a method for embedding a message within a file comprising:

generating a random key (content key 64; para. 0088);

encrypting the random key to produce an encrypted random key (content key encrypted with secret key 47; para. 0089);

encrypting the message (content information 41 in discrete data unit 44) to produce an encrypted message (para. 0087 and 0088); and

embedding the encrypted random key and the encrypted message in the file (para. 0090 and 0091).

But Hirano does not explain at least one of the encrypted random key and the encrypted message being embedded in random locations throughout the file.

However, Rhoads teaches a method for embedding a message within a file (col. 32, lines 37-40; col. 52, lines 23-26) wherein at least one of the encrypted random key and the encrypted message are embedded in random locations throughout the file for the purpose of hiding the message (a plurality of code words 216, each serving either as a key or a message, are embedded in random locations to look like noise; col. 4, lines 11-14; col. 12, lines 21-24; col. 18, line 52; col. 21, lines 36-61; col. 24, lines 37-42).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Hirano with the teaching of Rhoads such that at least one of the encrypted random key and the encrypted message being embedded in random locations throughout the file. One would be motivated to do so in order to enhance security since a potential attacker would not overtly recognize a hidden message.

Regarding claim 2, the modified method of Hirano and Rhoads is relied upon as applied to claim 1, and Hirano and Rhoads further teach that the generating includes generating a random symmetric encryption key (Hirano, content key 64 used for both encryption and decryption of the message; para. 0088). Therefore, for the reasons applied above, such a claim also would have been obvious.

Regarding claim 3, the modified method of Hirano and Rhoads is relied upon as applied to claim 1, and Hirano and Rhoads further teach that the encrypting the random

key includes asymmetrically encrypting the random key with an intended recipient's public key (Hirano, secret key 47 used to encrypt content key 64 is public key of the intended recipient; para. 0089 and 0098). Therefore, for the reasons applied above, such a claim also would have been obvious.

Regarding claim 4, the modified method of Hirano and Rhoads is relied upon as applied to claim 2, and Hirano and Rhoads further teach that the encrypting the random key includes asymmetrically encrypting the random key with an intended recipient's public key (Hirano, para. 0088). Therefore, for the reasons applied above, such a claim also would have been obvious.

Regarding claim 5, the modified method of Hirano and Rhoads is relied upon as applied to claim 1, but the modified method of Hirano and Rhoads does not explicitly explain compressing the message to obtain a compressed message prior to the encrypting the message.

However, Rhoads further teaches compressing the message to obtain a compressed message for the purpose of storage economy (col. 9, lines 19-20). Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Hirano with the further teaching of Rhoads to provide the step of compressing the message to obtain a compressed message prior to the encryption of the message. One would be motivated to do so for storage economy.

Regarding claim 6, the modified method of Hirano and Rhoads is relied upon as applied to claim 5, and Hirano and Rhoads further teach encrypting a length of the encrypted message with the random key to obtain an encrypted message length

(image-compositing information 65 containing message length (size) is encrypted with secret key 47; para. 0076 and 0089). Therefore, for the reasons applied above, such a claim also would have been obvious.

Regarding claim 7, the modified method of Hirano and Rhoads is relied upon as applied to claim 6, but the modified method of Hirano and Rhoads does not explicitly explain verifying that the file has sufficient capacity to contain the encrypted message length, the encrypted random key, and the encrypted message.

However, Rhoads further teaches verifying that a file has sufficient capacity to contain all the information to be embedded within it (all embedded information must be proportionally smaller in size than the file in which it is embedded in order to keep the additive noise below an acceptability threshold so as not to noticeably distort the original information in the file; col. 4, lines 12-40; col. 16, lines 1-8; col. 17, lines 29-31; col. 26, lines 12-34; col. 32, lines 48-51).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Hirano with the further teaching of Rhoads to provide the step of verifying that a file has sufficient capacity to contain the encrypted message length, the encrypted random key, and the encrypted message. One would be motivated to do so in order to avoid noticeably distorting the original information in the file.

Regarding claim 8, the modified method of Hirano and Rhoads is relied upon as applied to claim 1, but Hirano and Rhoads do not explain randomly embedding both the encrypted random key and the encrypted message throughout the file.

However, Rhoads further teaches that all embedded information is embedded in random locations throughout the file for the purpose of hiding the fact that the original file has been modified to contain embedded information (a plurality of code words 216 are embedded in random locations to look like noise; col. 4, lines 11-14; col. 12, lines 21-24; col. 16, lines 1-8; col. 18, line 52; col. 21, lines 36-61; col. 24, lines 37-42). Rhoads also teaches that a code word (216) can serve as a message or a key (col. 32, lines 34-40; col. 35, lines 27-29; col. 59, lines 52-55; col. 65, lines 7-15). One of ordinary skill in the art would recognize that the embedded information represents an encrypted message and an encrypted key where two code words are utilized to represent each respectively.

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Hirano with the further teaching of Rhoads to provide the step of randomly embedding both the encrypted random key and the encrypted message throughout the file. One would be motivated to do so in order to hide the fact that the original file has been modified to contain embedded information, particularly where a potential attacker would be alerted to the presence of embedded information were some of the embedded information embedded in non-random locations causing a noticeable distortion in the original file.

Regarding claim 9, the modified method of Hirano and Rhoads is relied upon as applied to claim 1, but Hirano and Rhoads do not explain seeding a random number generator with an intended recipient's public key, and supplementally seeding the random number generator with the random key.

However, Rhoads further teaches seeding a random number generator with a key for the purpose of reducing the information necessary to be stored at the time of embedding that would facilitate later decoding of the embedded information (col. 21, lines 15-22). One of ordinary skill in the art would recognize that any key would suffice to seed the random number generator so long as the key was available to both the sender and the recipient and that using a set of two keys is functionally equivalent to using a set of one key, as each set merely provides a different seed number.

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Hirano with the further teaching of Rhoads to provide the step of seeding a random number generator with an intended recipient's public key, and supplementally seeding the random number generator with the random key. One would be motivated to do so in order to reduce the information necessary to be stored at the time of embedding that would facilitate later decoding of the embedded information and the recipient's public key and the random key (content key) are the best choices for the seed because they are retained anyway.

Regarding claims 9 and 10, such claims are rejected for the same reasons as applied above to the modified method of Hirano and Rhoads of claim 9 and, therefore, also would have been obvious.

Regarding claim 12-18, these claims are rejected for the reasons as applied above to the modified method of Hirano and Rhoads of claims 1-11 and, therefore, also would have been obvious.

Regarding claim 19, the modified method of Hirano and Rhoads is relied upon as applied to claim 15, including embedding the encrypted message at locations in the file corresponding to random numbers generated by the random number generator after the supplementally seeding the random number generator with the random key, but Hirano and Rhoads do not explicitly explain that embedding the encrypted message occurs until a total number of bits embedded equals a predetermined percentage of available space within the file. However, the Examiner takes official notice that one of ordinary skill would recognize that where a predetermined percentage is equal to the fixed percentage of 100%, the entirety of the embedded information is placed randomly within the file. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to provide that embedding the encrypted message occurs until a total number of bits embedded equals a predetermined percentage of available space within the file. One would be motivated to do so in order to avoid noticeably distorting the original information in the file.

Regarding claims 21-23 and 25, these claims are rejected for the reasons as applied above to the modified method of Hirano and Rhoads of claims 1-11 and 19 and, therefore, also would have been obvious.

Regarding claim 25, the modified method of Hirano and Rhoads is relied upon as applied to claim 23, but Hirano and Rhoads do not explicitly explain that the determined percentage is a fixed percentage.

Regarding claim 27, this is a computer-readable-medium version of the claimed method above (claims 1, 9 and 10), wherein all limitations have been addressed. Therefore, for reasons applied above, such a claim also would have been obvious.

Regarding claim 28, this is a processing-device version of the claimed method above (claim 1), wherein all limitations have been addressed. Therefore, for reasons applied above, such a claim also would have been obvious.

Allowable Subject Matter

3. **Claims 20, 24 and 26 are objected to** as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

The following is a statement of reasons for the indication of allowable subject matter:

Regarding claims 20 and 24, the closest prior art, the modified method of Hirano and Rhoads, does not explain randomly embedding the encrypted message until a total number of bits embedded equals a predetermined percentage of available space within the file and then embedding the encrypted message at sequential unused locations in the file when the total number of bits embedded exceeds the predetermined percentage of available space within the file. The prior art first verifies that the file exhibits the capacity to contain the embedded information and then places the entirety of the embedded information in the file, with all segments of the embedded information placed at random locations. It would not be obvious to one of ordinary skill in the art to

first place a percentage of the embedded information randomly within the file and then to place the remainder in sequential order at unused locations because a non-random distribution of embedded information increases the likelihood of its discovery by potential attackers.

Regarding claim 26, the closest prior art, the modified method of Hirano and Rhoads, does not explain randomly embedding the encrypted message until a total number of bits embedded equals a predetermined percentage of available space within the file, wherein the predetermined percentage is randomly determined. The prior art first verifies that the file exhibits the capacity to contain the embedded information and then places the entirety of the embedded information in the file, with all segments of the embedded information placed at random locations. It would not be obvious to one of ordinary skill in the art to place less than the entirety of the embedded information randomly within the file because a non-random distribution of embedded information increases the likelihood of its discovery by potential attackers.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to John Elmore whose telephone number is 571-272-4224. The examiner can normally be reached on M 10-8, T-Th 9-7.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on 571-272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

JE

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100